

Blaine J. Benard (#5661)
Brent E. Johnson (#7558)
Engels J. Tejeda (#11427)
Emily T. Howe (#18294)
HOLLAND & HART LLP
222 South Main Street, Suite 2200
Salt Lake City, UT 84101-2194
Telephone: 801.799.5800
bjbenard@hollandhart.com
bjohnson@hollandhart.com
ejtejeda@hollandhart.com
ethowe@hollandhart.com

Attorneys for Defendant Uintah Basin Healthcare

**IN THE UNITED STATES DISTRICT COURT,
IN AND FOR THE DISTRICT OF UTAH, CENTRAL DIVISION**

JASON RASMUSSEN et al., on behalf of
themselves and all others similarly situated,

Plaintiffs,

vs.

UINTAH BASIN HEALTHCARE, a Utah non-
profit corporation,

Defendant.

**DECLARATION OF PRESTON MARX IN
SUPPORT OF DEFENDANT’S MOTION
TO DISMISS PLAINTIFFS’ COMPLAINT
UNDER FEDERAL RULES OF CIVIL
PROCEDURE 12(b)(1) AND 12(b)(6) OR
IN THE ALTERNATIVE, SUMMARY
JUDGMENT UNDER RULE 56**

2:23-cv-00322-HCN-DBP

Judge Howard C. Nielson, Jr.
Chief Magistrate Judge Dustin B. Pead

I, Preston Marx, declare as follows:

1. I have personal knowledge of the facts, except only where noted they are based upon publicly available information, in this declaration and, if called to testify as a witness, I would testify under oath as to these facts.

2. The statements made herein are based upon my personal knowledge and upon my review of relevant records, documents, and information.

3. I am the Vice President of Strategy & Innovation at Uintah Basin Healthcare (“UBH”). I have worked for UBH in different capacities for almost 18 years.

4. UBH is an independent 49-bed hospital located in Duchesne County, Utah, a remote area located in the northeast section of the state.

5. UBH employs approximately 900 individuals, some of whom have access to patients’ personally identifiable information (“**PII**”) and protected health information (“**PHI**”) on an as needed basis.

6. UBH serves primarily local patients who live in Duchesne, Uintah, and Daggett Counties.

7. Attached as **Ex. 15** is a table created from addresses patients provide to UBH’s registration department. This data was regularly made, recorded and kept in the course of UBH’s regularly conducted business, was gathered at or near the time that the patients provided it, and was gathered by persons whose responsibility was to accurately record the data in the ordinary course of UBH’s business.

8. In 2020, 97.89% of UBH patients provided Utah addresses. *See* Ex. 15.

9. In 2021, 98.30% of UBH patients provided Utah addresses. *See* Ex. 15.

10. In 2022, 98.43% of UBH patients provided Utah addresses. *See* Ex. 15.

11. As of September 27, 2023, 98.57% of UBH patients provided Utah addresses. *See* Ex. 15.

12. Based on publicly available information, as of 2020, 74% of the housing units in Duchesne County were occupied by the owner. See <https://datausa.io/profile/geo/duchesne-county-ut?sexAgeRacePoverty=raceGenderOption#economy>

13. Based on publicly available information, 13.9% of the population in Duchesne County live below the poverty line. See <https://datausa.io/profile/geo/duchesne-county-ut?sexAgeRacePoverty=raceGenderOption#economy>

14. These statistics align with my personal experience while working and living in Duchesne County.

15. The statistics are consistent with UBH's assessment that it serves mostly Utah citizens who are domiciled in or around Duchesne County because UBH provides continuity care to many families, including extended families, who do not report having second homes in the area.

16. On November 7, 2022, UBH sustained a cybersecurity attack that locked up some of UBH's computer systems and held data hostage by a threat actor who demanded a ransom (the "**Incident**").

17. As of the date of the Incident, UBH had adopted a written information security program (the "**WISP**") that included over a dozen policies and protocols regarding information security, including the following:

- a. ITS Security Policy 1.4; a copy of which is attached as **Ex. 2**;
- b. ITS Network Management Policy 2.2; a copy of which is attached as **Ex. 3**;
- c. ITS Acceptable Use Policy 3.1; a copy of which is attached as **Ex. 4**;

- d. ITS Employee Account Policy 4.2; a copy of which is attached as **Ex. 5**;
- e. ITS Remote Access Policy 5.0; a copy of which is attached as **Ex. 6**;
- f. ITS Business Continuity Policy 7.1; a copy of which is attached as **Ex. 7**;
- g. ITS Asset Inventory Policy 8.0; a copy of which is attached as **Ex. 8**;
- h. ITS Incident Response Policy 9.0; a copy of which is attached as **Ex. 9**;
- i. ENG Physical Facilities Access Policy; a copy of which is attached as

Ex. 10;

- j. UBH Breach Notification Policy; a copy of which is attached as **Ex. 11**.

18. As of the date of the Incident, I was serving as the Security Officer under the WISP.

19. As UBH's Security Officer, I oversaw implementation of and compliance with the WISP.

20. As of the date of the Incident, UBH was in substantial compliance with the WISP's policies and protocols.

21. UBH engaged Intraprise Health – an outside, independent certified consultant – to conduct annual assessments of UBH's WISP from 2015 to 2022.

22. A true copy of Intraprise's 2021 assessment of UBH's WISP, redacted to protect highly sensitive cybersecurity information, is attached as **Ex. 12**.

23. A true copy of Intraprise's 2022 assessment of UBH's WISP, redacted to protect highly sensitive cybersecurity information, is attached as **Ex. 13**.

24. Intraprise attested that between 2021 and 2022, which included the date of the Incident, UBH's WISP complied with the Health Insurance Portability and Accountability Act of

1996 (“**HIPAA**”), 45 C.F.R. Part 164 Subpart C and the applicable provisions of NIST Special Publication 800-53 and 800-53a.

25. Copies of Intraprise’s certifications that UBH’s WISP complied with HIPAA in 2021 and 2022 are attached as **Ex. 14**.

26. Periodically, and at all times relevant to this lawsuit, UBH has taken steps to amend its policies and protocols to comply with recommendations made in the Intraprise assessments and to keep up with cybersecurity developments including regular updates to software security technology and recommended patches provided by UBH’s software vendors.

27. In addition, through UBH’s contract with the Utah Education and Telehealth Network, weekly system vulnerability scans were conducted on UBH’s circuits and edge equipment prior to and after the Incident.

28. Prior to and after the Incident, UBH adopted several risk mitigation protocols and processes, including standardizing operating systems for workstations, conducting monthly cybersecurity training for the information technology staff and quarterly anti-phishing testing and training for all staff, and deploying new technologies like network segmentation and monitoring software when they became available.

29. On November 7, 2022, UBH retained an outside forensic consultant to help UBH contain, investigate, and respond to the Incident.

30. On November 7, 2022, the outside consultant engaged with the threat actor on behalf of UBH.

31. On November 9, 2022, UBH confirmed the viability of its data backups and initiated restoration and recovery of the same.

32. On November 16, 2022, UBH reported the Incident to the Federal Bureau of Investigation.

33. On December 13, 2022, the threat actor provided UBH's consultant a decryption tool and represented it would restore all information potentially affected by the Incident.

34. On or around April 7, 2023, UBH determined the personal and protected health information of patients that received care with UBH between March 2020 and November 2022 may have been accessed or acquired without authorization during the Incident.

35. Although there is no evidence that the threat actor misused or published any data as a result of the Incident, UBH decided to notify all patients who received care between March 2012 and November 2022 about the Incident.

36. UBH hired a third party, Identity Theft Guard Solutions, Inc., d/b/a IDX to notify the patients. IDX submitted all names and addresses to the National Change of Address databank to secure current addresses. IDX confirmed that 91,950 of the 103,974 individuals who received care between March 2012 and November 2022 had Utah addresses.

37. On May 10, 2023, UBH notified the potentially affected individuals of the Incident.

38. An example of the notice sent to potentially affected individuals is attached as **Ex. 1.**

39. UBH does not retain patient payment card data on its system and its investigations have not revealed that payment card data was exposed or potentially exposed during the Incident.

I declare under penalty of perjury under the laws of the State of Utah and the United States that the foregoing is true and correct.

Executed this 16th Day of October, 2023.

/s/ Preston Marx
Preston Marx, UBH Security Officer

30716866_v1